

(e)

ELECTRONIC MONEY

Patent Number: JP9128464
Publication date: 1997-05-16
Inventor(s): HIRASAWA MASANORI
Applicant(s): KOKUSAI GIJUTSU KAIHATSU KK
Requested Patent: ☐ JP9128464
Application Number: JP19950286187 19951102
Priority Number(s):
IPC Classification: G06F19/00; G07F7/08; G09C1/00; H04L9/10
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To prevent appropriation of cash information by wiretap of communication by receiving and paying money from/to external equipment by means of a communication means.
SOLUTION: The electronic money 10 consists of two LSI chips for communication. LSI-B 12 executes first cipher information communication except for the exchange of cash information and outputs a command for giving instruction for reception or payment of money. On the other hand, LSI-A 11 records cash information and executes second cipher information communication for receiving and paying money from/to the external equipment based on the received command. In the period of this second cipher information communication, LSI-B 12 executes signal passage processing. The two pieces of cipher information makes it difficult to decipher a ciphered code. If the second cipher information communication is made an unopened system in particular, it is extremely difficult to decipher cipher information even though the wire is tapped.

Data supplied from the esp@cenet database - 12

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-128464

(43) 公開日 平成9年(1997)5月16日

(51) IntCl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 19/00			G 0 6 F 15/30	3 6 0
G 0 7 F 7/08		7259-5 J	G 0 9 C 1/00	6 6 0 C
G 0 9 C 1/00	6 6 0		G 0 7 F 7/08	J
H 0 4 L 9/10			H 0 4 L 9/00	6 2 1 Z

審査請求 未請求 請求項の数11 O L (全 18 頁)

(21) 出願番号 特願平7-286187

(22) 出願日 平成7年(1995)11月2日

(71) 出願人 000170554

国際技術開発株式会社

東京都杉並区天沼2丁目3番9号

(72) 発明者 平澤 正憲

埼玉県所沢市花園一丁目24番地の13

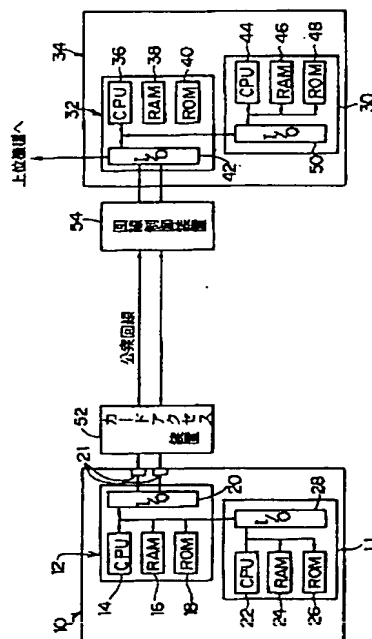
(74) 代理人 弁理士 中島 淳 (外2名)

(54) 【発明の名称】 電子マネー

(57) 【要約】

【課題】 通信手段により外部機器に対して入金、出金等の処理を行い、通信の盗聴による現金情報の盗用を防止する。

【解決手段】 電子マネーを2つの通信用LSIチップで構成する。LSI-Bは、現金情報の送受以外の第1の暗号化情報通信を行うと共に、入金や出金を指令するためのコマンドを出力する。一方、LSI-Aは、現金情報を記録すると共に、受信したコマンドに基づいて外部機器に対する入金や出金を行う第2の暗号化情報通信を行う。この第2の暗号化情報通信の間は、LSI-Bは、信号通過処理を行う。2つの暗号化情報により暗号化コードの解析は困難となる。特に第2の暗号化情報通信を未公開の方式とすれば、通信が盗聴されても暗号化情報の解析はきわめて困難となる。



【特許請求の範囲】

【請求項1】 現金情報に関する暗号化データを外部機器と通信することにより前記外部機器に対する入金又は出金を行う電子マネーであって、前記外部機器と前記現金情報の送受以外の第1の暗号化情報通信を制御すると共に、前記現金情報の入金又は出金のためのコマンドを出力する第1の通信手段と、現金情報が記録可能でかつ、前記コマンドを入力した場合には、前記コマンドに基づき前記第1の暗号化情報通信とは異なる第2の暗号化情報通信を前記外部機器と行うことによって前記外部機器に対する入金又は出金を制御する第2の通信手段と、を有することを特徴とする電子マネー。

【請求項2】 前記第1の通信手段は、前記現金情報の入金又は出金のためのコマンド以外に、少なくとも前記外部機器の有する現金情報の残高チェックのためのコマンド又は前記入金若しくは出金が正常に終了したか否かの状態問い合わせのコマンドを出力すると共に、前記第2の通信手段は、受信したコマンドに基づいて、前記外部機器との第2の暗号化情報通信を行うことを特徴とする請求項1の電子マネー。

【請求項3】 前記第2の通信手段は、前記外部機器との第2の暗号化情報通信を複数回行うことを特徴とする請求項1又は請求項2の電子マネー。

【請求項4】 前記第2の通信手段は、前記第2の通信手段により記録されている現金情報の残高を検出すると共に、前記第2の通信手段により検出された残高が信号として出力される出力端と、をさらに有することを特徴とする請求項1乃至請求項3のいずれか1項の電子マネー。

【請求項5】 前記第2の通信手段は、現在の年月日又は時刻を検出する日付手段と、前記日付手段により検出された年月日又は時刻が、予め設定された有効期限に達した時、前記第2の通信手段への入金を禁止し、少なくとも前記第2の通信手段からの出金を可能とする禁止手段と、をさらに有することを特徴とする請求項1乃至請求項4のいずれか1項の電子マネー。

【請求項6】 前記第2の通信手段は、前記コマンドに基づく通信回数を検出する回数検出手段と、前記回数検出手段により検出された通信回数が予め設定された使用頻度を越えた場合、前記第2の通信手段への入金及び出金を禁止する禁止手段と、をさらに有することを特徴とする請求項1乃至請求項5のいずれか1項の電子マネー。

【請求項7】 前記第2の通信手段は、前記現金情報へのアクセスがエラーとなった頻度を検出するエラー頻度検出手段と、

前記エラー頻度検出手段により検出されたエラーの頻度が予め設定されたエラー頻度を越えた場合、前記第2の通信手段からの出金を禁止する禁止手段と、をさらに有することを特徴とする請求項1乃至請求項6のいずれか1項の電子マネー。

【請求項8】 前記第2の通信手段は、前記入金又は出金の履歴を記録する履歴手段と、前記履歴手段により記録された前記入金又は出金の履歴が信号として出力される出力端と、をさらに有することを特徴とする請求項1乃至請求項7のいずれか1項の電子マネー。

【請求項9】 前記第1の通信手段は、予め登録されたアクセス先に対してのみ前記入金又は出金を可能とする限定手段と、をさらに有することを特徴とする請求項1乃至請求項8のいずれか1項の電子マネー。

【請求項10】 前記第1の通信手段は、使用者を特定するための暗号コードを有し、入力された番号が前記暗号コードと一致した場合にのみ、前記コマンドによる前記現金情報へのアクセスを可能とする認証手段と、

をさらに有することを特徴とする請求項1乃至請求項9のいずれか1項の電子マネー。

【請求項11】 前記第2の暗号化情報通信が未公開であることを特徴とする請求項1乃至請求項10のいずれか1項の電子マネー。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報として記録された現金を有し、該現金に関する暗号化データを外部機器と通信することにより現金情報の入金又は出金を行うICカード等の電子マネーに係り、特に防犯機能のさらなる向上を図った電子マネーに関する。

【0002】

【従来の技術】従来、預金口座への現金の入金や他の口座への現金の出金等を自動的に行うシステムとして銀行等に設置されている現金自動支払いシステムがある。

【0003】この現金自動支払いシステムでは、銀行が預金者に発行したプラスチック製の磁気カード、所謂キャッシュカードを介して取引ができるようになっていいる。この磁気カードには、預金者である使用者の指定口座番号等の所定の情報が磁気的に記録されており、使用者がこのカードを現金自動支払いシステムに挿入し、予めシステムに登録された暗証番号を入力すると、システムは、カードに記録されている口座番号等を読み出し、この口座番号に対応する登録暗証番号と入力された番号とが一致するか否かを判定する。そして、暗証番号が一致した時のみ、現金の払出し等の処理を行うようになっている。

【0004】

【発明が解決しようとする課題】しかしながら、上記従来の技術では、預金者が銀行や自動支払いサービスコーナー等に出向かなければ処理することができず、また、磁気カードそのものには現金としての機能がなく、このため銀行が現金を扱う量を減らすことができない、という問題点が生じる。

【0005】本発明は上記事実を考慮し、情報として記録された現金を有し、通信手段を介して現金の入金、出金等の処理を行うことができると共に、通信の盗聴による現金情報の盗用を防止した電子マネーを提供することが目的である。

【0006】

【課題を解決するための手段】以上のような課題を解決するため、請求項1の発明は、現金情報に関する暗号化データを外部機器と通信することにより前記外部機器に対する入金又は出金を行う電子マネーにおいて、前記外部機器と前記現金情報の送受以外の第1の暗号化情報通信を制御すると共に、前記現金情報の入金又は出金のためのコマンドを出力する第1の通信手段と、現金情報が記録可能でかつ、前記コマンドを入力した場合には、前記コマンドに基づき前記第1の暗号化情報通信とは異なる第2の暗号化情報通信を前記外部機器と行うことによって前記外部機器に対する入金又は出金を制御する第2の通信手段と、を有することを特徴とする。

【0007】請求項1の発明では、第1の通信手段が、外部機器と現金情報の送受以外の第1の暗号化情報通信を制御すると共に、現金情報の入金又は出金のためのコマンドを出力する。ここで、入金とは、電子マネーから外部機器へのお金を払い、電子マネー側からみた場合、現金情報の出金を意味する。また、出金とは、外部機器から電子マネーへのお金を払い、電子マネー側からみた場合、現金情報の入金を意味する。そして、第2の通信手段は、現金情報が記録可能であると共に、第1の通信手段からのコマンドを入力した場合には、当該コマンドに基づき第1の暗号化情報通信とは異なる第2の暗号化情報通信を外部機器と行うことによって外部機器に対する入金又は出金を制御する。ここで、第1の通信手段及び第2の通信手段を各々LSIチップで構成することができる。また、第2の暗号化情報通信の間は、第1の通信手段を構成するLSIチップで信号通過処理を行うようにしても良い。

【0008】以上のように、本発明では、通信によって遠隔にある外部機器との入金、出金の取引が可能となる。また、第1の通信手段による第1の暗号化情報通信と、第2の通信手段による第2の暗号化情報通信という互いに異なる暗号化方式を用い、しかも暗号化方式の切り換え時を外部から判定することが困難であるので、暗号化情報を解析することはきわめて困難となり、防犯効果が向上する。

【0009】請求項2の発明は、請求項1の前記第1の

通信手段が、前記現金情報の入金又は出金のためのコマンド以外に、少なくとも前記外部機器の有する現金情報の残高チェックのためのコマンド又は前記入金若しくは出金が正常に終了したか否かの状態問い合わせのコマンドを出力すると共に、請求項1の前記第2の通信手段が、受信したコマンドに基づいて、前記外部機器との第2の暗号化情報通信を行うことを特徴とする。

【0010】請求項2の発明では、第1の通信手段が、外部機器の有する現金情報の残高チェックのためのコマンド又は入金若しくは出金が正常に終了したか否かの状態問い合わせのコマンドを出力する。そして、第2の通信手段が入力したコマンドに基づいて外部機器との第2の暗号化情報通信を行う。これにより、入金又は出金以外に、通信によって銀行口座の残高チェックや状態問い合わせが可能となる。

【0011】請求項3の発明は、請求項1又は請求項2の前記第2の通信手段が、前記外部機器との第2の暗号化情報通信を複数回行うことを特徴とする。

【0012】請求項3の発明では、第2の通信手段が、外部機器との第2の暗号化情報通信を複数回行う。この複数回のデータ送受によって、暗号化情報の機密性が高まり、防犯効果のさらなる向上が得られる。

【0013】請求項4の発明は、請求項1乃至請求項3のいずれか1項の前記第2の通信手段が、前記第2の通信手段により記録されている現金情報の残高を検出すると共に、前記第2の通信手段により検出された残高が信号として出力される出力端と、をさらに有することを特徴とする。

【0014】請求項4の発明では、第2の通信手段が現金情報の残高を検出し、残高の信号を出力端から出力する。この残高の信号を表示すれば、当該電子マネーにおける現金情報の残高を直ちに知ることができる。

【0015】請求項5の発明は、請求項1乃至請求項4のいずれか1項の前記第2の通信手段が、現在の年月日又は時刻を検出する日付手段と、前記日付手段により検出された年月日又は時刻が、予め設定された有効期限に達した時、前記第2の通信手段へのお金を禁止し、少なくとも前記第2の通信手段からの出金を可能とする禁止手段と、をさらに有することを特徴とする。

【0016】請求項5の発明では、日付手段が現在の年月日又は時刻を検出する。そして、禁止手段は、検出された年月日又は時刻が、予め設定された有効期限に達した時、第2の通信手段へのお金を禁止し、少なくとも第2の通信手段からの出金（払出し）を可能とするように制御する。

【0017】請求項6の発明は、請求項1乃至請求項5のいずれか1項の前記第2の通信手段が、前記コマンドに基づく通信回数を検出する回数検出手段と、前記回数検出手段により検出された通信回数が予め設定された使用頻度を越えた場合、前記第2の通信手段へのお金及び

出金を禁止する禁止手段と、をさらに有することを特徴とする。

【0018】請求項6の発明では、回数検出手段がコマンドに基づく前記第2の通信手段の通信回数を検出する。そして、禁止手段は検出された通信回数が予め設定された使用頻度を越えた場合、第2の通信手段への入金及び出金を禁止するように制御する。

【0019】請求項7の発明は、請求項1乃至請求項6のいずれか1項の前記第2の通信手段が、前記現金情報へのアクセスがエラーとなった頻度を検出するエラー頻度検出手段と、前記エラー頻度検出手段により検出されたエラーの頻度が予め設定されたエラー頻度を越えた場合、前記第2の通信手段からの出金を禁止する禁止手段と、をさらに有することを特徴とする。

【0020】請求項7の発明では、エラー頻度検出手段が現金情報へのアクセスがエラーとなった頻度を検出し、禁止手段は、検出されたエラーの頻度が予め設定されたエラー頻度を越えた場合、第2の通信手段からの出金を禁止するように制御する。

【0021】請求項5～請求項7の発明により、防犯効果がさらに向上する。請求項8の発明は、請求項1乃至請求項7のいずれか1項の前記第2の通信手段が、前記入金又は出金の履歴を記録する履歴手段と、前記履歴手段により記録された前記入金又は出金の履歴が信号として出力される出力端と、をさらに有することを特徴とする。

【0022】請求項8の発明では、履歴手段が入金又は出金の履歴を記録し、出力端から記録された履歴信号を出力する。これによって、外部機器と離れた箇所でも入金及び出金の履歴を直ちに知ることができる。

【0023】請求項9の発明は、請求項1乃至請求項8のいずれか1項の前記第1の通信手段が、予め登録されたアクセス先に対してのみ出金を可能とする限定手段と、をさらに有することを特徴とする。

【0024】請求項9の発明は、請求項1乃至請求項8のいずれか1項の前記第1の通信手段が、予め登録されたアクセス先に対してのみ前記入金又は出金を可能とする限定手段と、をさらに有することを特徴とする。

【0025】請求項9の発明では、限定手段は、予め登録されたアクセス先に対してのみ入金又は出金を可能とするように制御する。

【0026】請求項10の発明は、請求項1乃至請求項9のいずれか1項の前記第1の通信手段が、使用者を特定するための暗号コードを有し、入力された番号が前記暗号コードと一致した場合にのみ、前記コマンドによる前記現金へのアクセスを可能とする認証手段と、をさらに有することを特徴とする。

【0027】請求項10の発明では、電子マネーは使用者を特定するための暗号コードを有しており、認証手段が入力された番号が暗号コードと一致した場合にのみ、

前記コマンドによる前記現金へのアクセスを可能とするように制御する。

【0028】このように電子マネー自体に認証機能を付加することにより、防犯効果はさらに向上する。

【0029】請求項11の発明は、請求項1乃至請求項10のいずれか1項の前記第2の暗号化情報通信が未公開であることを特徴とする。

【0030】請求項11の発明では、未公開の第2の暗号化情報通信が行われる。これにより、暗号化データの解析はさらに困難となり、さらに防犯効果を向上させることができる。

【0031】

【発明の実施の形態】本発明の実施の形態を図1乃至図16にしたがって説明する。

【0032】図1に、本発明の実施の形態に係る電子マネー10と外部機器34の構成、及びこれらの機器が公衆回線によって接続されている状態を示す。なお、外部機器34として、例えば現金自動支払いシステムや自動販売機等がある。

【0033】図1に示すように、本実施の形態に係る電子マネー10は、LSIチップ11（以下、LSI-Aという）及びLSIチップ12（以下、LSI-Bという）を含んだ所謂ICカードとして構成されている。ここで、LSI-Aは、情報としての現金（現金情報）を記録すると共に、現金情報の出し入れを管理・制御するための電子財布としての機能を有する。このLSI-Aは、LSIチップ全体の管理・制御を実行するCPU22と、現金情報を記録するためのRAM24と、ROM26と、I/Oポート28と、から構成されており、各々がデータやコマンドを伝達するためのバスによって接続されている。なお、電子マネー10に電源が内蔵されていない場合には、電源の供給がオフになったとしても記録された現金情報が失われないようにRAM24として、データのリード/ライトが可能な不揮発性メモリが用いられる。

【0034】また、ROM26には、制御用のプログラムが格納されており、CPU22は、このプログラムに基づいて、LSI-Bから出力されてきたコマンドを解析し、該コマンドに基づいて外部機器34との通信制御を実行し、RAM24に記録された現金情報の入金や出金等の制御を行う。

【0035】また、図16に示すように、LSI-AのI/Oポート28には、年月日又は時刻をカウントするクロック27が接続されており、CPU22は、クロック27によりカウントされた年月日又は時刻を検知できるようになっている。

【0036】また、I/Oポート28には、光を検出する光センサー29が接続されており、光センサー29が光を検出すると、検出信号をCPU22に伝達する。なお、光センサー29は、LSI-Aのケーシングの外部

に配置されている。さらに、I/Oポート28には、予備電源13が接続されており、本来の電源が供給されていない場合でも、光センサー29が光を検出した場合には、CPU22やRAM24等へ電源が供給されるようになっている。

【0037】一方、LSI-Bは、外部機器34との通信のインターフェイス制御を行うと共に、LSI-Aを制御するための複数種類のコマンドを出力する。このインターフェイス制御では、外部機器34の種類に応じて通信を制御するようになっている。

【0038】図1に示すように、LSI-Bは、LSIチップ全体の管理・制御を実行するCPU14と、外部機器34から送られてきたデータが記憶されるRAM16と、ROM18と、I/Oポート20と、から構成されており、各々がデータやコマンドを伝達するためのバスによって接続されている。また、このバスには、LSI-AのI/Oポート28が接続されている。

【0039】また、I/Oポート20には、図示しない電源、後述するカードアクセス装置52及び外部機器34との信号の受け取り受渡しを行うための電気接点21が接続されている。

【0040】また、ROM18には、制御用のプログラムが格納されており、CPU14は、このプログラムに基づいて外部機器34との通信制御を実行し、外部機器34から送られてきた暗号化データを解読し、解読されたデータに基づいて、入金や出金等を行うためのコマンドをLSI-Aに出力する。

【0041】また、電子マネー10は、公衆回線にアクセスして外部機器34と接続するためのカードアクセス装置52を介して外部機器34と通信を行うようになっている。このカードアクセス装置52の詳細な構成を図2に示す。図2に示すように、カードアクセス装置52は相手先との通信に必要な情報や電子マネー10への指令等を入力するためのキーボード66及び電気接点21から出力された入金、出金の履歴、電子財布等の残高情報を表示するディスプレイ68を備え、内部には電子マネー10を内部へ搬送する搬送装置70が設けられている。搬送装置70は、所定の間隔に配設された挟持ローラー対72、74を備え電子マネー10を挟持して、図2の矢印A方向及び矢印A方向とは反対方向に搬送する。

【0042】挟持ローラー対72と挟持ローラー対74の間には、電子マネー10の電気接点21に接触する接触端子76が設けられている。

【0043】この接触端子76はI/Oポート64を介して公衆回線との接続を制御する回線制御装置60及びモデム62に接続されている。さらに接触端子76には、カードアクセス装置52の図示しない電源が接続されており、該電源の供給によって電子マネー10が動作するようになっている。

【0044】一方、外部機器34は、公衆回線の接続の制御を行う回線制御装置54を介して電子マネー10と接続されている。

【0045】外部機器34は、電子マネー34と同様にLSIチップ30（以下、LSI-A' という）及びLSIチップ32（以下、LSI-B' という）の2つのLSIチップを含んで構成されている。

【0046】ここで、外部機器34が現金自動支払いシステムの場合、LSI-A' は、RAM46に口座毎に記録された現金情報（電子預金）の出し入れを管理する機能を有する。なお、RAM46として、電子マネー10のRAM24と同様に、不揮発性メモリを使用しても良い。

【0047】また、LSI-B' のI/Oポート42には、ホストコンピュータ等の上位機種が接続されており、口座に関する情報等をやり取りできるようになっている。なお、上記以外のLSI-A' 及びLSI-B' の構成及び機能は、各々電子マネー10のLSI-A及びLSI-Bとほぼ同様であり、詳細な説明を省略する。

【0048】次に、電子マネー10と外部機器34との通信処理の概要を図3によって説明する。

【0049】図3に示すように、まずLSI-BとLSI-B' との間で所定の手順に従って第1の暗号化情報通信を行う（ステップ90）。この通信では、電子マネー10が外部機器34と現金情報に関する取引を行う上で必要となる情報が、相手先の外部機器34に送信される。

【0050】ところで、LSI-BとLSI-B' との間の通信では、防犯効果を高めるために送信するコードにスクランブルをかけて暗号化している。

【0051】次に、この暗号化方法について説明する。例えば送信するコードの列が例えば64ビットであるとする。

【0052】64ビットのコードは、所定の方法で例えば8ビット×8列のマトリックスに変更され、各行、各列が所定の方法にしたがってそれぞれローテートされる。ローテートされたマトリックス状のコードは再び所定の方法で64ビット列にされ、暗号化が完了する。

【0053】本実施の形態では、8ビット×8列のマトリックスにされたコードの各行、各列のローテートの回数及び8ビット×8列のマトリックスにされたコードを64ビット一列にする方法のそれぞれを変えることによって、複数個の暗号化方法を得ている。

【0054】なお、暗号化の方法を選択するにあたっては、それぞれの暗号化の方法に番号を付し、暗号化の方法の番号に応じた乱数を発生させるようにすればよい。例えば、暗号化の方法が100通りあったとすると、各暗号化の方法に1～100までの番号を付して暗号化方法と共に暗号化テーブル（図15参照）としてROM1

8に記憶しておく。

【0055】さらにLSI-B及びLSI-B'では、CPU14及びCPU36によりシードデータに基づいて乱数が生成されるようになっており、乱数を暗号化の方法の番号に対応させて1~100までの何れか1つを生成するようにする。暗号化するに当たっては、その時に生成された乱数に対応した暗号化方法にしたがって送信するコードを暗号化する。なお、暗号化されたデータには、所定の位置に、暗号化の方法を示す暗号化コードを付け加える。

【0056】一方、復号側にも、暗号側と同様の暗号化テーブルが記憶されており、復号は、暗号化コードに基づいて暗号化の逆の手順で行う。即ち、64ビットの暗号化されたコードが、暗号化と逆の手順にしたがって8ビット×8列のマトリックスに戻され、各行、各列がそれぞれ上記と逆にローテートされ、再び64ビット一列にされて元のコードが得られる。

【0057】図3のステップ90の通信が終了すると、外部機器34においてLSI-BからLSI-B'に送出された情報が正しい情報であるか否かが判定される(ステップ92)。情報が正しいと判定された場合(ステップ92肯定判定)にのみ次のステップ94に進み、情報に誤りがある場合(ステップ92否定判定)には、通信処理を終了する。

【0058】ステップ94では、LSI-B及びLSI-B'が現金情報の出し入れ等を制御するためのコマンドを生成し、各々LSI-A及びLSI-A'に出力する(ステップ94)。なお、LSI-BとLSI-Aの間の通信、LSI-BとLSI-A'の間の通信では、暗号化情報を用いない通常の通信を用いても良い。

【0059】次に、LSI-B及びLSI-B'が各々信号通過処理を行う(ステップ96)。すなわち、LSI-B、B'が各々のバスをLSI-A、A'に開放すると共に、通信制御を一時的に停止する。この処理によって、LSI-A、LSI-A'との間で異なる通信手順に従った独自の通信が可能となる。

【0060】次に、LSI-AとLSI-A'との間で伝送されたコマンドに基づき現金情報等のコードを暗号化して第2の暗号化情報通信を行う(ステップ98)。この第2の暗号化情報通信では、LSI-B、B'間の第1の暗号化情報通信とは異なる暗号化方式が用いられる。本実施の形態では、複数回の通信に分割して第2の暗号化情報通信を行うことにより、暗号化の強度を高めている。ここで、コードを暗号化する方法としては、周知の方法を適用することができるが、特に非公開の暗号化方式を用いる方が防犯効果の点で好ましい。

【0061】以上のように、LSI-B、B'間の第1の情報化通信と、LSI-A、A'間の第2の情報化通信という互いに異なる暗号化方式を用い、しかも暗号化方式の切り換え時を外部から判定することが困難であるの

で、暗号コードを解析することはきわめて困難となる。

【0062】次に、LSI-A、A'、LSI-B、B'の各々の処理の流れについて図4乃至図7のフローチャートによって詳細に説明する。なお、以下の説明では、外部機器34が現金自動支払いシステムの場合を扱う。

【0063】まず、LSI-Bの処理について図4によって説明する。図4に示すように、LSI-Bへの入力を待機し(ステップ100否定判定)、入力があった場合(ステップ100肯定判定)、入力信号がフラグリセット信号以外の信号であるか否かを判定する(ステップ102)。

【0064】入力信号がフラグリセット信号以外の信号である場合(ステップ102肯定判定)、フラグF₁が0であるか否かを判定し(ステップ104)、フラグF₁が0の場合に(ステップ104肯定判定)、入力信号の情報をRAM16に記憶する(ステップ106)。

【0065】次に、RAM16に記憶された情報を読み出し、暗号化コードに変換する(ステップ108)。そして、前述した第1の暗号化情報通信を外部機器34のLSI-B'と実行する(ステップ110)。この通信によって、例えば電子マネー10にキーボード66を介して入力された口座番号、当該口座の暗唱番号、及びIDコードが相手先の外部機器34(現金自動支払いシステム)に送信される。また、この暗号化情報通信では、入金、出金、残高チェック等の旨が送信される。なお、IDコードは、当該電子マネー10を特定するためのコード番号であり、図14に示すように、通常では書き込み等のアクセスが禁止されているメモリ領域に予め登録されているものである。

【0066】次に、LSI-B'からの許可信号の受信を待機し(ステップ112否定判定)、許可信号を受信した場合(ステップ112肯定判定)、LSI-Aへコマンドを出力する(ステップ114)。このコマンドは、ステップ100で入力された情報に基づいて決定され、例えば次のような4種類の機能①~④を各々有するコマンドのいずれか1つが出力される。

【0067】① 電子預金から電子マネーへの入金(入金コマンド)

② 電子預金から電子マネーへの出金(出金コマンド)

③ 電子預金の残高チェック(残高チェックコマンド)

④ 通信の状態(入金等が正常に終了したか、アラームが発生したか否か、電子預金の残高が足らなかったか否かの状態)の問い合わせ(状態問い合わせコマンド)

なお、①~④の機能を有するコマンドは、図13に示すように各々が特定の命令コードによって表される。

【0068】次に、フラグF₁に1を代入し、再びステップ100で入力信号を待機する(ステップ116)。

【0069】一方、フラグF₁が0でなかった場合(ステップ104否定判定)、前述した信号通過処理を実行

し(ステップ118)、再びステップ100で入力信号を待機する。

【0070】また、フラグリセット信号が入力された場合(ステップ102否定判定)、ステップ118の信号通過処理を解除し(ステップ120)、フラグ F_1 に0を代入し(ステップ122)、ステップ100で入力信号を待機する。

【0071】次に、LSI-B'の処理について図5によって説明する。図5に示すように、LSI-B'への入力を待機し(ステップ130否定判定)、入力があった場合(ステップ130肯定判定)、入力信号がフラグリセット信号以外の信号であるか否かを判定する(ステップ132)。

【0072】入力信号がフラグリセット信号以外の信号である場合(ステップ132肯定判定)、フラグ F_2 が0であるか否かを判定し(ステップ134)、フラグ F_2 が0の場合には(ステップ134肯定判定)、入力信号の暗号化コードを復号化する(ステップ136)。

【0073】次に、復号化された情報が正しいか否かを判定する(ステップ138)。例えば、復号化情報から電子預金の口座番号と、暗証番号を読み出し、予めROM40に登録されている当該口座の暗証番号が受信された暗証番号と一致した場合、に情報が正しいと判定する。

【0074】復号化情報が正しくないと判定した場合(ステップ138否定判定)、再びステップ130に戻り、入力信号を待機する。一方、復号化情報が正しいと判定した場合には(ステップ138肯定判定)、LSI-Bへ許可信号を送出し(ステップ140)、LSI-A'へコマンドを出力する。このコマンドは、LSI-Bから送られてきた暗号化情報に記録されている入金、出金等の別に基づいて、各々に対応する処理をLSI-A'に実行させるためのものである。すなわち、当該コマンドは、図4のステップ114でLSI-AからLS

- ① 入金コマンド : 入金予定額 M_{in} の送信
- ② 出金コマンド : 出金予定額 M_{out} の送信
- ③ 残高チェックコマンド : 電子預金口座の残高 m の受信
- ④ 状態問い合わせコマンド : 状態情報の受信

ここで、前述したように第2の暗号化情報通信では、暗号化コードを複数回に分割して通信を行っているので、公衆回線への侵入者が M_{in} や M_{out} 等の金額を盗聴することはきわめて困難となる。

【0082】第2の暗号化通信が終了すると(ステップ170で肯定判定)、コマンド別に各々の処理を実行する。

【0083】入金コマンドの場合(ステップ172肯定判定)、通信が正常に終了したか否か、すなわちLSI-A'に入金予定額 M_{in} が正常に伝達されたか否かを判定する(ステップ174)。この判定は、LSI-A'から送られてきた入金正常終了のフラグ信号を解析する

LSI-A'へ出力されたコマンドに各々対応する。

【0075】次に、フラグ F_2 に1を代入し、再びステップ130で入力信号を待機する(ステップ116)。

【0076】一方、フラグ F_2 が0でなかった場合(ステップ134否定判定)、前述した信号通過処理を実行し(ステップ146)、再びステップ130で入力信号を待機する。

【0077】また、フラグリセット信号が入力された場合(ステップ132否定判定)、ステップ146の信号通過処理を解除し(ステップ148)、フラグ F_2 に0を代入し(ステップ150)、ステップ130で入力信号を待機する。

【0078】次に、LSI-Aの処理について図6のフローチャートによって説明する。図6に示すように、まず、LSI-BからLSI-Aへのコマンド入力を待機する(ステップ160否定判定)。コマンドが入力された場合(ステップ160肯定判定)、入力コマンドを判別する(ステップ162)。

【0079】コマンドが入金コマンド又は出金コマンドである場合(ステップ164肯定判定)、入金予定額 M_{in} 又は出金予定額 M_{out} を読み出す(ステップ166)。図13に示すように、入金コマンド及び出金コマンドの場合には、各々のコマンドコードに入金予定額 M_{in} 、出金予定額 M_{out} のコードが付加されており、ステップ166では、このコードを読み出す処理を行う。入金コマンド及び出金コマンド以外のコマンドの場合(ステップ164否定判定)には、当該処理を行わない。

【0080】次に、LSI-A'との第2の暗号化通信を実行する(ステップ168)。この通信では、コマンド毎に次のような情報のやり取りが行われる。なお、受信された暗号化コードは予め記憶された復号化方式に従い復号化される。

【0081】

ことによって行われる。

【0084】通信が正常に終了した場合(ステップ174肯定判定)は電子預金への入金が完了した場合であるので、LSI-Aの電子財布に記録されている残高 M から入金額 M_{in} を引いた値を残高 M とする(ステップ176)。

【0085】また、出金コマンドの場合(ステップ178肯定判定)、通信が正常に終了したか否かを判定し(ステップ180)、通信が正常に終了した場合には(ステップ180肯定判定)、さらに電子預金の口座に M_{out} 以上の残金があったか否かをLSI-A'からの受信信号を解析することにより判定する(ステップ18

2)。

【0086】電子預金の口座に M_{out} 以上の残金がある場合(ステップ182肯定判定)、LSI-Aの電子財布に記録されている残高 M から電子預金からの出金額 M_{out} を加算した値を残高 M とする(ステップ184)。通信が正常に終了しなかった場合(ステップ180否定判定)又は口座に M_{out} 以上の残金が無かった場合(ステップ182否定判定)には、残高 M への M_{out} の加算を行わない。

【0087】また、残高チェックコマンド又は状態問い合わせコマンドの場合(ステップ178否定判定)、LSI-Aからの受信データに記録されている残高 m 又は状態情報の読み出し、記憶を行う(ステップ186)。

【0088】各コマンド別の処理が終了すると、入出金の履歴がRAM24に記録される(ステップ188)。なお、この履歴記録では、LSI-A側の処理を履歴として記録する方法の他に、電子預金のLSI-A'から送られてきた当該口座における入出金の履歴を記録するようにしても良い。

【0089】次に、LSI-Bの信号通過処理を解除させるためのフラグリセット信号を出力し(ステップ190)、再びステップ160に戻りコマンド入力を待機する。

【0090】なお、電子マネー10では、キーボード66からの指令信号に基づいて、ステップ186で記憶された残高 m や状態情報、又はステップ188で記録された入出金履歴の信号を電気接点21を介して出力する。出力された残高 m や状態情報の信号は、ディスプレイ68上に表示され、オペレータは直ちにこれらの情報を知ることができる。

【0091】次に、LSI-A'の処理について図7のフローチャートによって説明する。図7に示すように、まず、LSI-B'からLSI-A'へのコマンド入力を待機する(ステップ200否定判定)。コマンドが入力された場合(ステップ200肯定判定)、入力コマンドを判別する(ステップ202)。

【0092】入力コマンドが残高チェックコマンドの場合(ステップ204肯定判定)、電子預金として記録されている指定口座の残高 m を検出する(ステップ206)。また、入力コマンドが状態問い合わせコマンドの場合(ステップ208肯定判定)、先の現金情報の通信時にCPU44によってRAM46に記録された状態情報を読み出す(ステップ210)。入金コマンド及び出金コマンドの場合(ステップ204否定判定及びステップ208否定判定)には、当該処理を行わない。

【0093】次に、LSI-Aとの第2の暗号化通信を実行する(ステップ212)。この通信は、図6のステップ168の通信に対応するもので、送受信されるデータが互いに逆の関係になっている。なお、受信された暗号化コードは予め記憶された復号化方式に従い復号化さ

れる。

【0094】第2の暗号化通信が終了すると(ステップ212肯定判定)、コマンド別に各々の処理を実行する。

【0095】入金コマンドの場合(ステップ216肯定判定)、通信が正常に終了したか否か、すなわちLSI-A'に入金予定額 M_{in} が正常に伝達されたか否かを判定する(ステップ174)。

【0096】通信が正常に終了した場合(ステップ216肯定判定)は、LSI-A'の電子財布に記録されている残高 m に入金額 M_{in} を加算した値を残高 m とする(ステップ220)。

【0097】また、出金コマンドの場合(ステップ22肯定判定)、通信が正常に終了したか否かを判定し(ステップ224)、通信が正常に終了した場合には(ステップ224肯定判定)、さらに残高 m が M_{out} 以上であるか否かを判定する(ステップ226)。

【0098】電子預金の口座に M_{out} 以上の残金がある場合(ステップ226肯定判定)、残高 m から出金額 M_{out} を引いた値を電子預金の残高 m とする(ステップ228)。通信が正常に終了しなかった場合(ステップ224否定判定)又は口座に M_{out} 以上の残金が無かった場合(ステップ226否定判定)には、当該口座からの M_{out} の出金を行わない。

【0099】また、状態問い合わせコマンドの場合(ステップ222否定判定)、ステップ212の第2の暗号化情報通信の通信履歴等に基づいて状態を検出し(ステップ231)、検出された状態情報を記憶する(ステップ232)。このLSI-Aからの受信データに記録されている残高 m 又は状態情報の読み出し、記憶を行う(ステップ186)。

【0100】各コマンド別の処理が終了すると、LSI-B'の信号通過処理を解除させるためのフラグリセット信号を出力し(ステップ234)、再びステップ200に戻りコマンド入力を待機する。

【0101】以上のように、電子マネー10は2つのLSIチップを有し、各々異なる暗号化方式を用いることによって侵入者を排除しているが、さらに防犯効果を高めるために、以下に述べるような複数の防犯処理が用意されている。これらの処理について図8乃至図12、及び図17のフローチャートにより説明する。

【0102】まず、有効期限設定処理を図8によって説明する。図8に示すように、電子マネー10を使用できる有効期限を設定する(ステップ240)。この設定では、例えばキーボード66によって有効期限を入力できるようにし、一度設定された有効期限を変更不可にする。登録された有効期限は、図14に示すように、メモリ領域の所定箇所に登録される。また、有効期限を入力不可とし、電子マネー10を使用した時点から予め登録された有効期限を設定するようにしても良い。

【0103】次に、年月日又は時刻を検出する（ステップ242）。この年月日等のカウントは、例えば図16のLSI-AのI/Oポート28に接続されたクロック27が行い、CPU22がそのカウント値を検知できるようになっている。

【0104】次に、ステップ242で測定された年月日又は時刻が、ステップ240で設定された有効期限に達したか否かをCPU22が判定する（ステップ244）。有効期限に達していない場合には（ステップ244否定判定）、再びステップ242に戻り、年月日又は時刻の測定を行う。

【0105】有効期限に達した場合（ステップ244肯定判定）、電子マネー10への入金を禁止し、電子マネー10からの払出しのみを可能とする（ステップ246）。なお、ステップ246の電子マネーへの入金の禁止は、図14に示すように、メモリ領域に記録されている禁止フラグ（0/1）の値に基づいて行われる。すなわち、LSI-Aは電子財布のRAM24へアクセスする場合、入金の禁止フラグ及び払出しの禁止フラグを参照し、禁止フラグが0の場合、電子財布への入金処理を可能とし、禁止フラグが1の場合には、電子財布への入金処理を禁止する。ステップ246の場合、入金の禁止フラグが1で、払出しの禁止フラグが0となるようにメモリ領域がアクセスされる。

【0106】以上のように電子マネー10の使用できる有効期限を設定できるようにしたので、電子マネー10を盗用された場合でも、被害を少なくすることができる。

【0107】次に、不正アクセス禁止処理を図9によって説明する。図9に示すように、まず、LSI-AのCPU22がエラー回数Eに0を代入する（ステップ248）。次に、電子財布への入金、出金等のアクセスを待機する（ステップ250否定判定）。

【0108】電子財布へのアクセスがあった場合（ステップ250肯定判定）、当該アクセスがエラー終了したか否かを判定する（ステップ252）。アクセスが正常終了した場合（ステップ252否定判定）、ステップ248に戻ってエラー回数に0を代入する。一方、電子財布へのアクセスがエラー終了した場合（ステップ252肯定判定）、Eを1インクリメントし（ステップ254）、Eが連続エラー回数のしきい値Th1を越えたか否かを判定する（ステップ256）。なお、連続エラー回数のしきい値Th1は、図14の示すように、メモリ領域の所定箇所に記録されている。Eがしきい値Th1を越えていない場合（ステップ256否定判定）、再びステップ250に戻り、電子財布へのアクセスを待機する。

【0109】Eがしきい値Th1を越えた場合（ステップ256肯定判定）、電子財布からの払出しを禁止する（ステップ258）。なお、この処理の場合には、図1

4の払出し禁止フラグが1に、入金フラグが0に設定される。

【0110】以上のように連続してTh1を越えたエラー回数が生じた場合には、電子マネー10の盗用者が電子マネーへのアクセス方法を調べている場合であるとみなし、LSI-Aが電子財布からの払出しを禁止することによって盗用の被害を未然に防止することができる。なお、ステップ258で電子財布からの払出しのみを禁止するようにしたが、電子財布への入金も禁止するようにしても良い。

【0111】次に、使用頻度制限処理を図10によって説明する。図10に示すように、まずLSI-AのCPU22が、時間tに0を代入し（ステップ260）、使用頻度Uに0を代入する（ステップ262）。

【0112】次に、時間をカウントするため、tを1インクリメントし（ステップ264）、tが使用頻度の検出期間のしきい値Th2を越えたか否かを判定する（ステップ266）。tがしきい値Th2を越えた場合（ステップ266肯定判定）、再びステップ260、262に戻り、t及びUを0クリアして同様の処理を繰り返す。

【0113】tがしきい値Th2を越えていない場合（ステップ266肯定判定）、電子財布へのアクセスがあったか否かを判定する（ステップ268）。電子財布へのアクセスが無かった場合（ステップ268否定判定）、ステップ264に戻り、時間tをカウントする。

【0114】電子財布へのアクセスがあった場合（ステップ268肯定判定）、Uを1インクリメントし（ステップ270）、Uが使用頻度のしきい値Th3を越えているか否かを判定する（ステップ272）。Uがしきい値Th3を越えていない場合（ステップ272否定判定）、ステップ264に戻り、時間tをカウントする。

【0115】Uがしきい値Th3を越えている場合には（ステップ272肯定判定）、電子財布へのアクセスを禁止する（ステップ274）。すなわち、電子サイフへの入金及び払出しの禁止フラグを1にする。

【0116】以上のように、エラー回数だけではなく、正常終了した場合のアクセス回数を含めた使用頻度が大きい場合に入金や払出しを禁止することによって、さらに徹底して盗用による被害を防止することができる。

【0117】次に、アクセス可能先設定処理を図11によって説明する。図11に示すように、まず、LSI-Bが相手先と暗号化情報通信を行い（ステップ280）、当該通信相手のID番号を受信する（ステップ282）。

【0118】次に、LSI-BのCPU14が、予め登録されたアクセス可能先のID番号の読み出しを行う（ステップ284）。なお、アクセス可能先のID番号は、図14に示すようにメモリ領域に予め登録されている。そして、通信相手がアクセス可能先であるか否かを

判定する(ステップ286)。すなわち、通信相手のID番号がアクセス可能先のID番号の中にあるか否かを判定する。

【0119】通信相手がアクセス可能先でなかった場合(ステップ286否定判定)、LSI-Aへコマンドを出力せず、入金、出金、及び残高チェック等の禁止処理を行う(ステップ290)。すなわち、入金、出金等の禁止フラグを1に設定する。なお、残高チェックに関しては図示しないが、入金、出金の禁止フラグと同様に禁止フラグを設けることができる。一方、通信相手がアクセス可能先である場合には(ステップ286肯定判定)、通常通り、入金、出金、及び残高チェック等の処理を実行する(ステップ288)。

【0120】次に、認証機能を図12によって説明する。図12に示すように、キーボード66を介して暗号コードをLSI-Bに入力する(ステップ300)。次に、メモリ領域に予め登録されている暗号コードの読み出しを行う(ステップ302)。

【0121】次に、LSI-BのCPU14が入力された暗号コードと登録されている暗号コードとが一致するか否かを判定する(ステップ304)。暗号コードが一致していなかった場合(ステップ304否定判定)、LSI-Aへコマンドを出力せず電子財布の入金、出金等の処理を禁止する(ステップ306)。

【0122】一方、暗号コードが互いに一致した場合には(ステップ304肯定判定)、この電子マネー10を特定するIDコードをメモリ領域から読み出し(ステップ308)、該IDコードに基づいて相手先と入金、出金等の処理を行う(ステップ310)。

【0123】以上のように、電子預金の口座の暗証番号のみならず、電子マネー自体にも使用者本人を認証するための機能を付与したので、防犯機能のさらなる向上が図られる。

【0124】次に、現金情報クリア処理を、図17によって説明する。図17に示すように、まず、LSI-AのCPU22が、図16に示された光センサー29からの出力信号に基づいて光センサー29が光を検出したか否かを判定する(ステップ320)。

【0125】光センサー29が光を検出しない場合(ステップ320否定判定)、そのまま待機し、通常の処理を続行する。光を検出した場合(ステップ320肯定判定)、CPU22がRAM24に記録された現金情報等をクリアする(ステップ322)。すなわち、RAM24に記録されている現金情報、暗号コード及び暗号コード用のパラメータ等がクリアされる。

【0126】なお、光センサー29が光を検出した場合には、予備電源13からLSI-Aへ電源が供給され、電子マネー10へカードアクセス装置52からの電源が供給されていない場合でも現金情報クリア処理が実行できるようになっている。

【0127】このように、LSI-Aの現金情報を引き出そうとする盗用者が、電子マネーを破壊しても、外部の光によって電子財布に記録された現金情報や暗号コード等がクリアされるので盗用を未然に防止することができる。

【0128】上記では、予備電源からLSI-Aへ電源を供給する例について説明したが、受光可能なように光センサーをLSI-Aに組み込むか、光センサーをLSI-Aの近傍に配置し、受光したときに光センサーから出力される光電流を利用して、RAMに記録されている情報をクリアするようにしてもよい。なお、光電流が微弱な場合もあるが、RAMに記録されている情報をクリアする場合には、少なくとも暗号コードに関連する情報がクリアできればよい。

【0129】以上が、本発明に係る電子マネー10の実施の形態であるが、上記例にのみ限定されるものではない。例えば、電子マネー10は図2に示されたカードアクセス装置52を介して外部機器34と通信可能としたが、電子マネー10に回線制御装置60やモデム62等を内蔵させて通信機能を備えたICカードとして構成しても良い。

【0130】また、通信手段に関して公衆回線に限定されるものではなく、データ等を送受信できる他の通信網、例えばインターネット等を用いることもできる。

【0131】さらに、現金情報の入金、出金の処理は現金自動支払いシステムにのみ適用されるのではなく、情報現金の送受信が可能な装置、例えば自動販売機等にも適用可能である。この場合、LSI-Bから出力されるコマンドも上記例に限られず、商品売る側の口座への現金振込等、アプリケーションに応じて用意される。

【0132】また、残高チェックコマンドで検出された預金残高をディスプレイ68に表示するようにしたが、LSI-Aが電子財布自体の残高を検出し、電気接点21を介して当該残高を出力し、ディスプレイ68に表示するようにしても良い。

【0133】また、図17の現金情報クリア処理において、光が検出された場合だけではなく、電子マネー10の図示しないケーシングが破壊された場合に、現金情報がクリアされるようにしても良い。

【0134】

【発明の効果】以上説明したように、請求項1～請求項11の発明によれば、通信手段を介して遠隔にある現金の入金、出金等の処理を行うことができると共に、通信の盗聴による現金情報の盗用を有効に防止できる、という効果が得られる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る電子マネーの構成及び電子マネーと公衆回線を介して通信を行う外部機の構成を示す図である。

【図2】カードアクセス装置の構成を示す図である。

【図3】本実施の形態に係る通信処理の概要を示すフローチャートである。

【図4】本実施の形態に係るLSI-Bの通信処理を示すフローチャートである。

【図5】本実施の形態に係るLSI-B'の通信処理を示すフローチャートである。

【図6】本実施の形態に係るLSI-Aの通信処理を示すフローチャートである。

【図7】本実施の形態に係るLSI-A'の通信処理を示すフローチャートである。

【図8】有効期限設定処理の流れを示すフローチャートである。

【図9】アクセス禁止処理の流れを示すフローチャートである。

【図10】使用頻度制限処理の流れを示すフローチャートである。

【図11】アクセス可能先設定処理の流れを示すフローチャートである。

【図12】認証機能の流れを示すフローチャートである。

る。

【図13】LSI-Bが出力するコマンドのコードの構成を示す図である。

【図14】登録された情報が記憶されているメモリ領域のデータ構成を示す図である。

【図15】暗号化テーブルのデータ構成を示す図である。

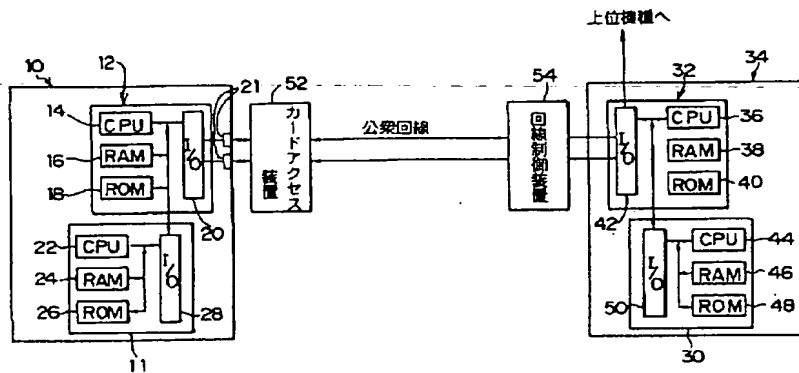
【図16】クロックを有するLSI-Aの構成を示す図である。

【図17】現金情報クリア処理の流れを示すフローチャートである。

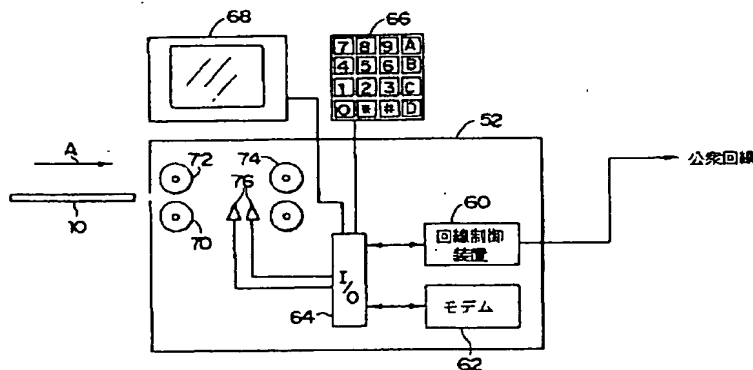
【符号の説明】

10 電子マネー
11 LSI-A
12 LSI-B
30 LSI-A'
32 LSI-B'
34 外部機器

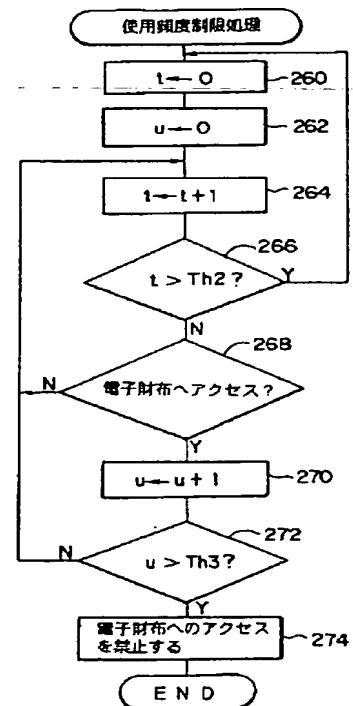
【図1】



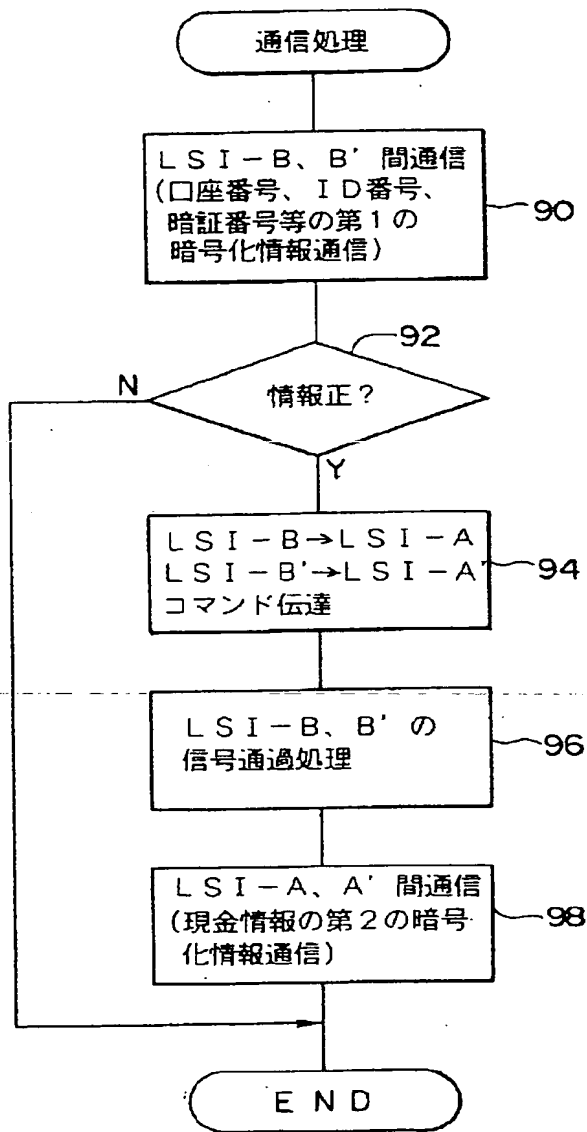
【図2】



【図10】



【図3】

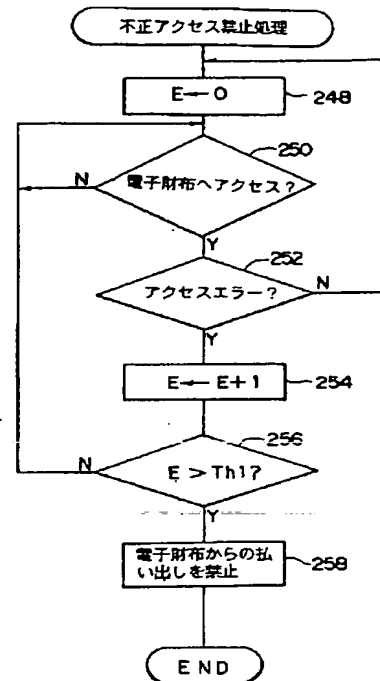


【図15】

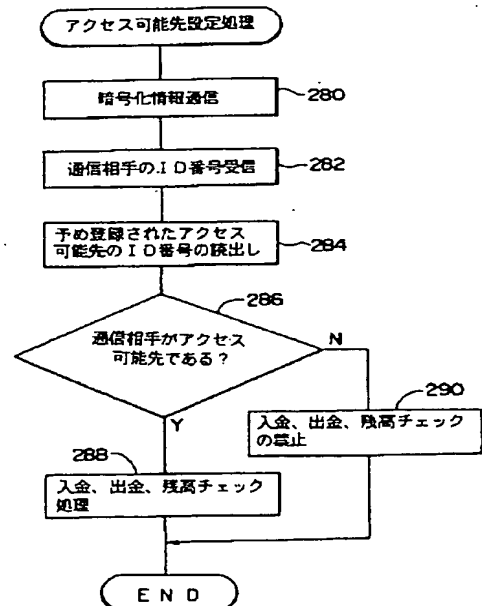
暗号化テーブル

番号	暗号化方法	暗号化コード
1	暗号化方法1	0000
2	暗号化方法2	0001
3	⋮	⋮
⋮	⋮	⋮

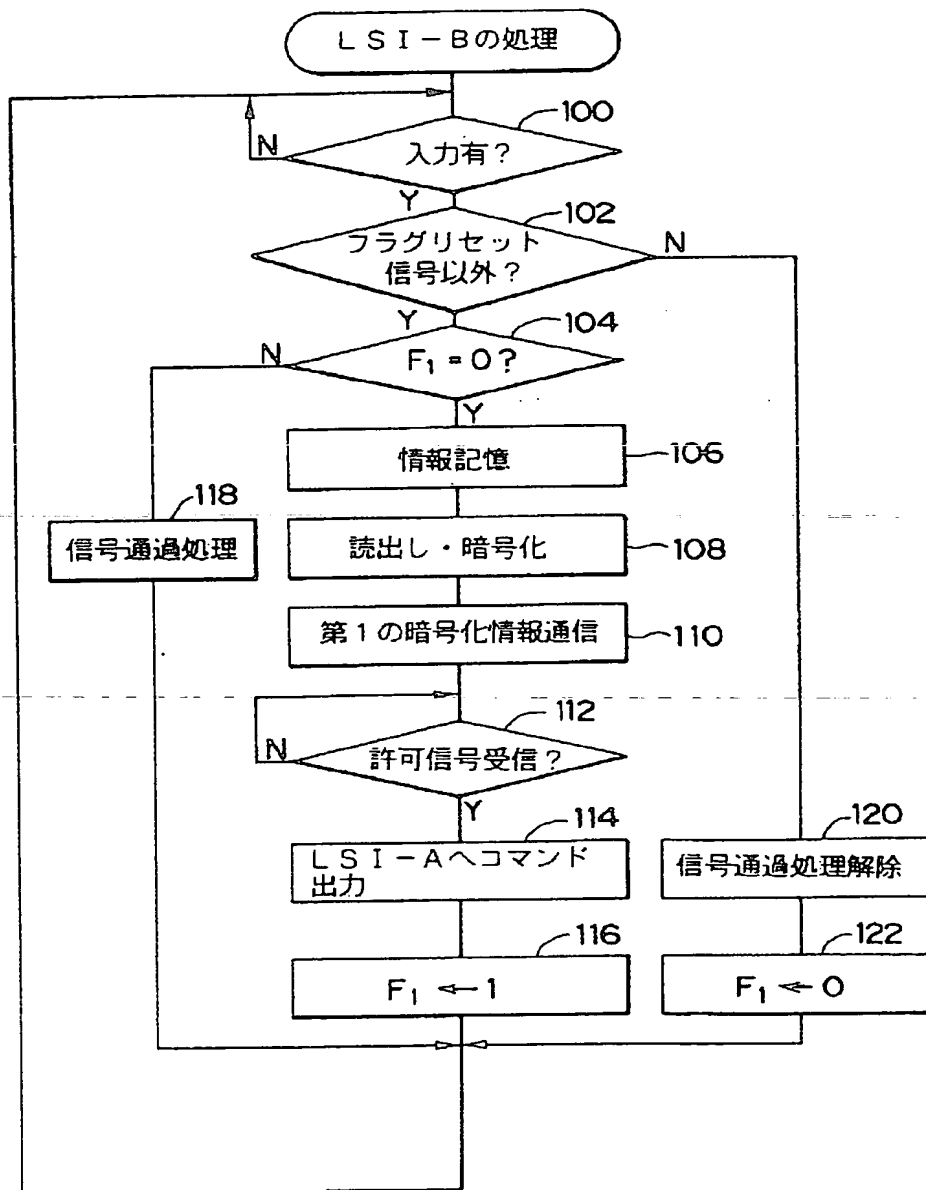
【図9】



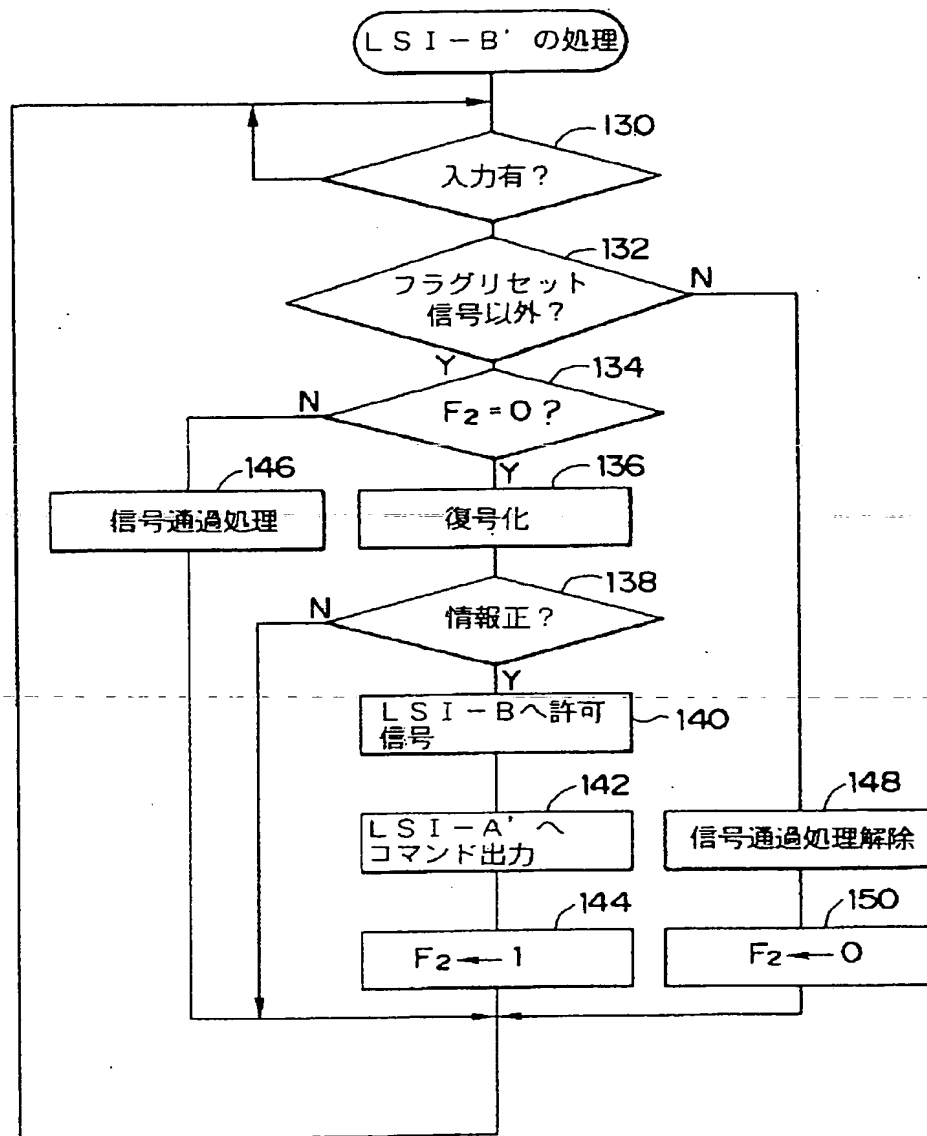
【図11】



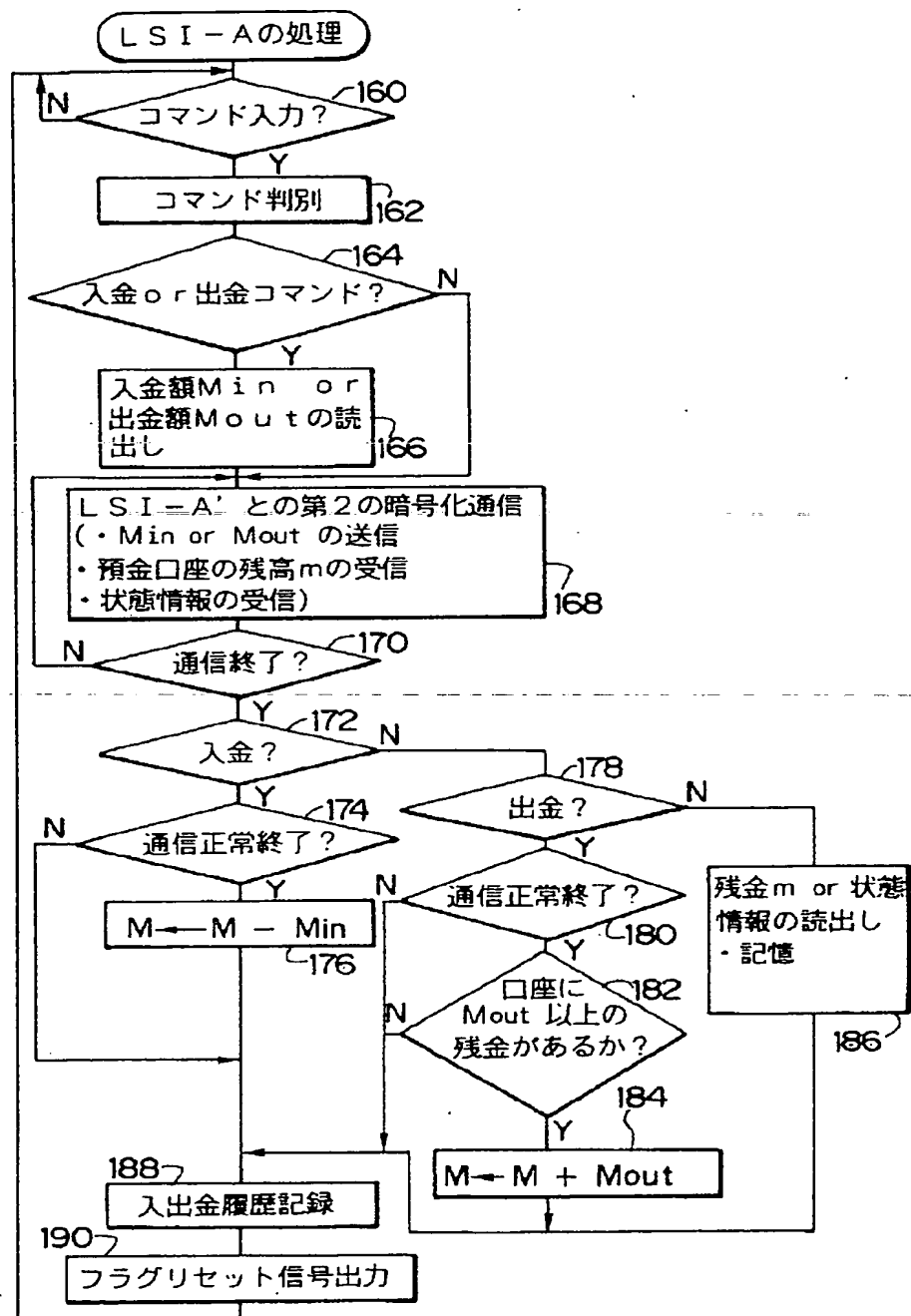
【図4】



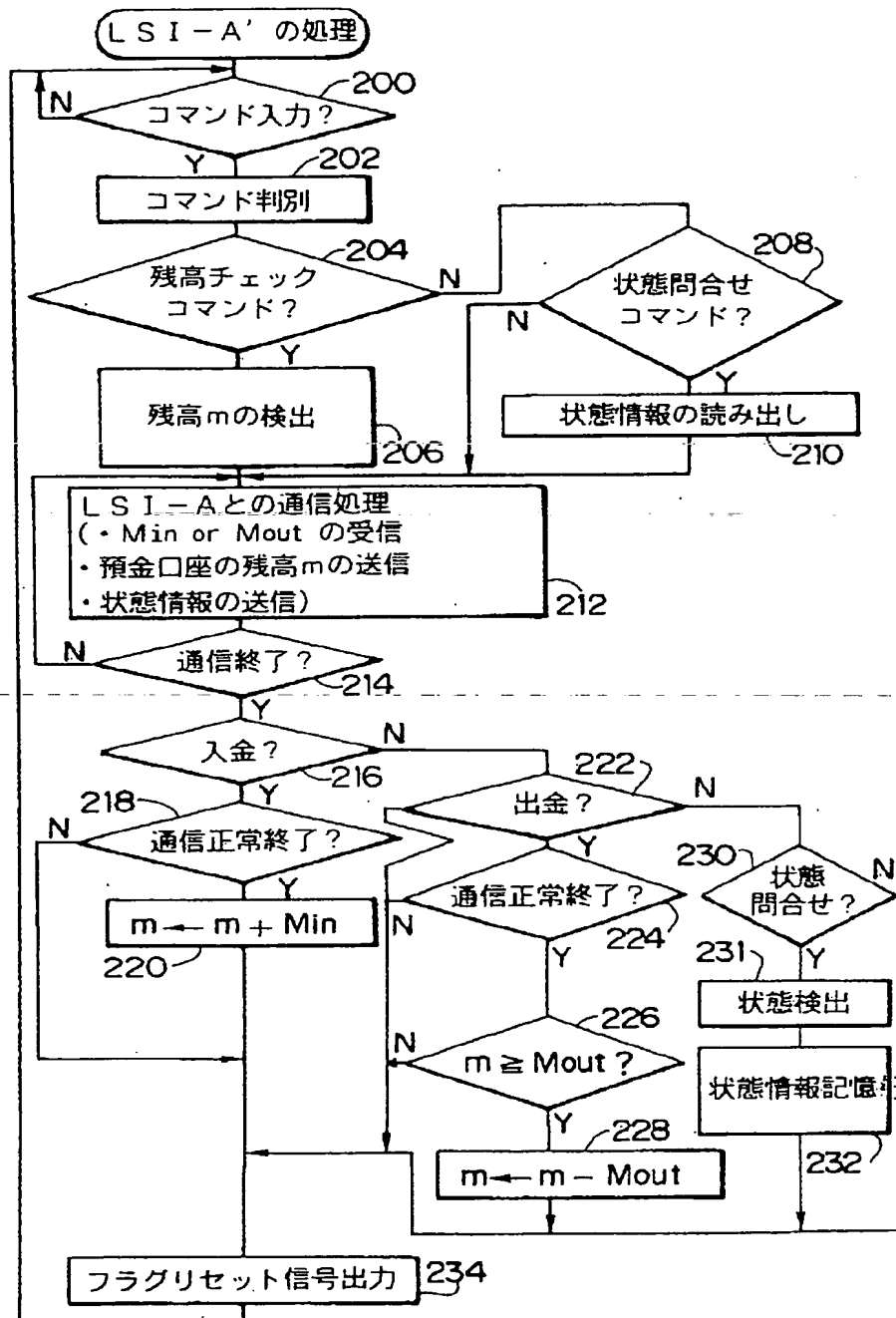
【図5】



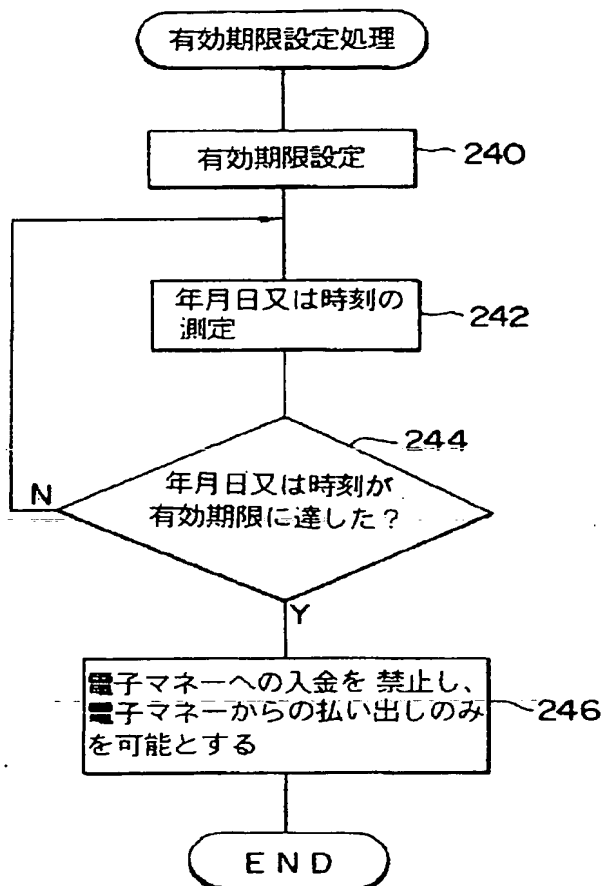
【図6】



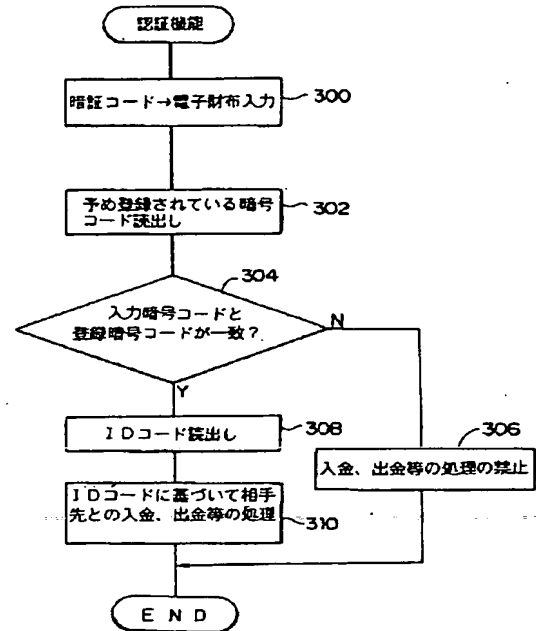
【図7】



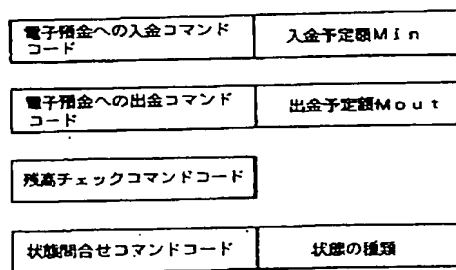
【図8】



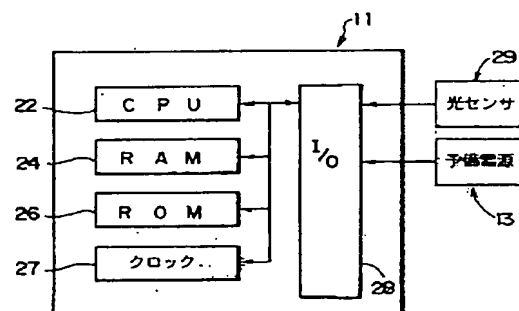
【図12】



【図13】



【図16】



【図14】

IDコード		メモリ領域
暗号コード		
電子マネーへの入金	禁止フラグ (0/1)	
電子マネーからの払出し	禁止フラグ (0/1)	
アクセス可能先数		
J R	ID番号0	
J H	ID番号1	
A B C	ID番号2	
⋮		
X Y Z	ID番号3	
有効期限		
連続エラー数のしきい値 Th 1		
使用頻度の検出期間のしきい値 Th 2		
使用頻度のしきい値 Th 3		

【図17】

